



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/594,299	09/26/2006	Yunchuan Qin	SHA-142NP	8794
23995	7590	04/17/2009	EXAMINER	
RABIN & Berdo, PC 1101 14TH STREET, NW SUITE 500 WASHINGTON, DC 20005			CHAL LONGBIT	
ART UNIT	PAPER NUMBER			
		2431		
MAIL DATE	DELIVERY MODE			
04/17/2009	PAPER			

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/594,299	<b>Applicant(s)</b> QIN ET AL.
	<b>Examiner</b> LONGBIT CHAI	<b>Art Unit</b> 2431

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If no period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED. (35 U.S.C. § 133).

Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

1) Responsive to communication(s) filed on 26 September 2006.

2a) This action is FINAL.      2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

4) Claim(s) 1-60 is/are pending in the application.

4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.

5) Claim(s) \_\_\_\_\_ is/are allowed.

6) Claim(s) 1-60 is/are rejected.

7) Claim(s) \_\_\_\_\_ is/are objected to.

8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on 26 September 2006 is/are: a) accepted or b) objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All    b) Some \* c) None of:

1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) Notice of References Cited (PTO-892)

2) Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) Information Disclosure Statement(s) (PTO/06/08)  
Paper No(s)/Mail Date \_\_\_\_\_

4) Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_

5) Notice of Informal Patent Application

6) Other: \_\_\_\_\_

**DETAILED ACTION**

***Priority***

1. Applicant's claim for benefit of foreign priority under 35 U.S.C. 119 (a) – (d) is acknowledged.

The application is filed on 9/26/2006 but is a 371 case of PCT/CN05/00368 application filed on 3/24/2005 and has a foreign priority application filed on 3/26/2004.

***Claim Objections***

2. Claims 1 is objected to because of the following informalities: "A secret file access authorization system with fingerprint limitation comprising the following components as follows:  
[[An]] an authorization server provided with an authorization module, which provides a fingerprint template and an authorization secret key[[.]];

[[An]] an encryption server provided with an encryption module, which generates a decryption secret key by accepting the authorization secret key provided by the authorization module, and produces the encrypted secret files by encrypting the secret files to be encrypted [[.]];

[[An]] a certification server provided with an the authorization module, which accepts the fingerprint template provided by the authorization module, accepts the decryption secret key provided by the encryption module and the authorization secret key claiming certification that is sent by the a client, and judges and confirms by providing the a certified decryption secret key [[.]];

[[At]] at least one client machine, each is provided with a user module, which embeds the a kernel encryption/decryption unit into the a corresponding operation system kernel of the client, accepts the authorization secret key provided by the authorization module and the decryption secret key provided by the encryption module, sends the claiming certification respectively to a certification module, .....". Any other claims not addressed by virtue of their dependency should also be corrected.

3. Claims 2 is objected to because of the following informalities: "the encryption server and the certification server are merged to constitute a system server, which is provided with the authorization module, the encryption module and the certification module" *should be replaced* with "the authorization server", the encryption server and the certification server are merged to constitute a system server, which is provided with the authorization module, the encryption module and the certification module". According to the specification, the disclosure indicates that the authorization server, the encryption server and the certification server can be merged into a system server, which is provided with the corresponding authorization module, encryption module and certification module (SPEC: Page 3 Line 14 – 16).

4. Claims 14 is objected to because of the following informalities: "the user module includes the an application unit, the kernel encryption/decryption unit and the an input/output unit, which are linked in sequence by the bidirectional programs; as well as the an authorization input unit, which accepts the authorization secret key and sends it into the kernel encryption/decryption unit; ..... Any other claims not addressed by virtue of their dependency should also be corrected.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1 – 60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Felsher (U.S. Patent 2002/0010679), which also contains, at least, Hillhouse (U.S. Patent 6,052,468) and Sudia (U.S. Patent 6,009,177) as being **incorporated by references**, in view of Tello (U.S. Patent 2003/0018892).

As per claim 1, Felsher teaches secret file access authorization system with fingerprint limitation comprising the components as follows:

**an authorization server provided with an authorization module, which provides a fingerprint template and an authorization secret key** (Hillhouse: Column 8 Line 23 – 26 / 46 – 65, Column 1 Line 40 – 45 and Column 5 Line 35 – 43: the key server is qualified as an authorization-and-encryption server);

**an encryption server provided with an encryption module, which generates a decryption secret key by accepting the authorization secret key provided by the authorization module, and produces the encrypted secret files by encrypting the secret files to be encrypted** (Hillhouse: Column 5 Line 42 – 43, Column 8 Line 23 – 26 / 46 – 65, Column 1 Line 40 – 45 and Column 5 Line 35 – 40);

**a certification server provided with an authorization module, which accepts the fingerprint template provided by the authorization module, accepts the decryption secret**

**key provided by the encryption module and the authorization secret key claiming certification that is sent by the client, and judges and confirms providing the certified decryption secret key** (Felsher: Para [0315] and [0198] & Hillhouse: Column 5 Line 35 – 43, Column 8 Line 23 – 26 / 46 – 65 and Column 1 Line 40 – 45);

at least one client machine, each is provided with a user module, which embeds the kernel encryption/decryption unit into the corresponding operation system kernel of the client (see Tello below), **accepts the authorization secret key provided by the authorization module and the decryption secret key provided by the encryption module** (Hillhouse: Column 5 Line 42 – 43, Column 8 Line 23 – 26 / 46 – 65, Column 1 Line 40 – 45 and Column 5 Line 35 – 40: see above), **sends the claiming certification respectively to certification module** (Sudia: Column 10 Line 50 – 53 and Column 15 Line 23 – 31), **opens the encryption / decryption unit with the certified authorization secret key and the certified decryption secret key which is returned after the certification module makes the certification, and reads/writes the encrypted secret files** (Felsher: Para [0119] Line 15 – 20, Para [0314] Line 9 – 11 and Para [0315]).

However, Felsher does not teach *embedding the kernel encryption / decryption unit into the corresponding operation system kernel of the client*.

Tello teaches **embedding the kernel encryption/decryption unit into the corresponding operation system kernel of the client** (Tello: Para [0200]).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Tello within the system of Felsher because (a) Felsher teaches the encryption / decryption key are used in a locally executing algorithm to encrypt / decrypt and release the file content (Felsher: Para [0233] Line 8 – 12), and (b) Tello teaches a more secured and cost-effective security kernel (i.e. the operating systems have an

encryption system embedded) that provides encryption / decryption in real time without requiring an extended resource from the main CPU (Tello: Para [0200]).

As per claim 2, Felsher as modified teaches the authorization server, the encryption server and the certification server are merged to constitute a system server, which is provided with the authorization module, the encryption module and the certification module (Hillhouse: Column 8 Line 23 – 26 / 46 – 65, Column 1 Line 40 – 45 and Column 5 Line 35 – 43: a key server is qualified as an authorization-and-encryption server) & (Felsher: Page 15 / Right Column / Line 49 – 50: centralizing processing of a key server and certification server for life cycle management where a key server is also qualified as an authorization-and-encryption server – i.e. centralized the certification server and authorization-and-encryption server are integrated and served as a system server).

As per claim 3, Felsher as modified teaches the authorization server and the encryption server are merged to constitute an authorization-and-encryption server, which is provided with the authorization module and the encryption module (Hillhouse: Column 8 Line 23 – 26 / 46 – 65, Column 1 Line 40 – 45 and Column 5 Line 35 – 43: a key server is qualified as an authorization-and-encryption server).

As per claim 4, Felsher as modified teaches the authorization server and the certification server are merged to constitute an authorization-and-certification server, which is provided with the authorization module and the certification module (Felsher: Para [0117] Line 7 – 13: a certification server is also an authorization server that can enable the client device to

communicate with other trusted devices).

As per claim 5, Felsher as modified teaches the encryption server and the certification server are merged to constitute an encryption-and-certification server, which is provided with the encryption module and the certification module (Felsher: Para [0315] Line 3 – 5 / Line 11 – 16: a certification is also a encryption / decryption server that can be driven by a need to account for access the release file content after decrypting the encrypted data file).

As per claim 6 and 17 – 20, Felsher as modified teaches the authorization module includes a password fingerprint unit, an environment fingerprint sampling unit and a time fingerprint sampling unit, which are set in parallel, as well as the authorization unit that is linked with the said three units which are set in parallel respectively by the bidirectional programs; the authorization unit provides the authorization secret key; while the password fingerprint unit, the environment fingerprint sampling unit and the time fingerprint sampling unit that are set in parallel provide the fingerprint template altogether (Felsher: Para [0087] Line 15 – 20: (a) the unique finger-print generating device is qualified as an environment fingerprint sampling unit and the finger-print digital information and (b) according to the present time when sampled, the time fingerprint sampling unit generates the unique and unduplicable data to be used as the time fingerprint) & (Hillhouse: Column 5 Line 42 – 43, Column 8 Line 23 – 26 / 46 – 65, Column 1 Line 40 – 45 and Column 5 Line 35 – 40: finger-print & passwords).

As per claim 7 and 21 – 24, Felsher as modified teaches the authorization secret key is a binary string of a certain length (Hillhouse: Column 8 Line 23 – 26 / 46 – 65, Column 1 Line 40

– 45 and Column 5 Line 35 – 43: the authorization key is derived from the user identity information (e.g. a password / finger-print is hashed into a 64-bit code).

As per claim 8 and 25 – 28, Felsher as modified teaches the authorization secret key can be put into the authorized entity (Hillhouse: Column 8 Line 23 – 26 / 46 – 65, Column 1 Line 40 – 45 and Column 5 Line 35 – 43).

As per claim 9 and 29 – 32, Felsher as modified teaches , the fingerprint template is a binary string of a certain length (Hillhouse: Column 6 Line 48 – 51: the fingerprint template is a binary string of a certain length in order to assure the derived crypto-key has a determinable key-length).

As per claim 10 and 33 – 36, Felsher as modified teaches the encryption module includes the secret key generation unit and the encryption unit, which are linked in sequence by the programs; the secret key generation unit provides the decryption secret key after accepting the authorization secret key provided by the authorization module; the encryption unit accepts the input of secret files to be encrypted, and produces the encrypted secret files by using the decryption secret key provided by the secret key generation unit (Hillhouse: Column 5 Line 42 – 43, Column 8 Line 23 – 26 / 46 – 65, Column 1 Line 40 – 45 and Column 5 Line 35 – 43: (a) the key server is qualified as an authorization-and-encryption server, which is provided with the authorization module and the encryption module (b) the registered user finger-print data is qualified as a set of fingerprint templates and (c) the authorization key is derived from the user identity information (e.g. a password / finger-print is hashed into a 64-bit code) which is used to encrypt the cryptographic key that encrypts the data file and (d) a cryptographic key is used to

encrypt the data file after being decrypted by an authorization key, which is derived from the user identity information).

As per claim 11 and 37 – 40, Felsher as modified teaches the encryption unit accepts the input of the secret files to be encrypted, and produces the encrypted secret files by using the authorization secret key (Hillhouse: Column 5 Line 42 – 43, Column 8 Line 23 – 26 / 46 – 65, Column 1 Line 40 – 45 and Column 5 Line 35 – 40: (a) the key server is qualified as an encryption-and-authorization server, which is provided with the encryption module and the authorization module; and (b) a cryptographic key is used to encrypt the data file after being decrypted by an authorization key, which is derived from the user identity information).

As per claim 12 and 41 – 44, Felsher as modified teaches the encryption unit accepts the input of the secret files to be encrypted, and produces the encrypted secret files by using the decryption secret key and the authorization secret key at the same time (Hillhouse: Column 5 Line 42 – 43, Column 8 Line 23 – 26 / 46 – 65, Column 1 Line 40 – 45 and Column 5 Line 35 – 40: a cryptographic key is used to encrypt the data file after being decrypted by an authorization key, which is derived from the user identity information and thereby, the decryption secret key and the authorization secret key must be used at the same time).

As per claim 13 and 45 – 48, Felsher as modified teaches the certification module includes an environment fingerprint certification unit, a password fingerprint certification unit, and a time fingerprint certification unit set in parallel by accepting the fingerprint template provided by the authorization module; the certification interface unit linked with them by the bidirectional programs, which also accepts the decryption secret key provided by the encryption

module and the certification secret key from the user module claiming certification respectively, and provides the certified decryption secret key for the user module (Felsher: Para [0087] Line 15 – 20: (a) the unique finger-print generating device is qualified as an environment fingerprint sampling unit and the finger-print digital information and (b) according to the present time when sampled, the time fingerprint sampling unit generates the unique and unduplicable data to be used as the time fingerprint) & (Hillhouse: Column 5 Line 42 – 43, Column 8 Line 23 – 26 / 46 – 65, Column 1 Line 40 – 45 and Column 5 Line 35 – 40: finger-print & passwords) & (Sudia: Column 10 Line 50 – 53 and Column 15 Line 23 – 31: the certification module validates the identity of the user prior to issuing the certificate).

As per claim 14 and 49 – 52, Felsher as modified teaches the user module includes the application unit, the kernel encryption/decryption unit and the input/output unit, which are linked in sequence by the bidirectional programs; as well as the authorization input unit, which accepts the authorization secret key and sends it into the kernel encryption/decryption unit; the kernel encryption/decryption unit provides the authorization secret key claiming certification for the certification module, and accepts the certified decryption secret key sent by the certification module; and the input/output unit is coupled with the encrypted secret files bidirectionally; the kernel encryption/decryption unit is embedded in the client operation system kernel (Tello: Para [0200]: the operating systems have an encryption system embedded in order to speed the encryption / decryption process in more secure way through the security engine, where the system includes a security kernel that provides encryption / decryption in real time without requiring an extended resource from the main CPU) & (Hillhouse: Column 5 Line 42 – 43, Column 8 Line 23 – 26 / 46 – 65, Column 1 Line 40 – 45 and Column 5 Line 35 – 40) & (Sudia: Column 10 Line 50 – 53 and Column 15 Line 23 – 31).

As per claim 15 and 53 – 56, Felsher as modified teaches the client operation system can be Microsoft Windows 95/98/ME/NT/2000/XP/2003 Server or Linux/Unix or Pocket, Symbian OS, Windows CE embedded operation system or Mac OS or Sun OS, Novell netware and other server or network operation systems (Tello: Para [0004]: Microsoft Windows 2000).

As per claim 16 and 57 – 60, Felsher as modified teaches the program used by the application unit can be Microsoft Office and its components or other desktop applications or embedded applications (Tello: Para [0004]: application that is running under Microsoft Office including Windows 2000).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LONGBIT CHAI whose telephone number is (571)272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Longbit Chai/

Longbit Chai E.E. Ph.D  
Primary Examiner, Art Unit 2431  
4/10/2009